User Account Management

User Account Management involves several features such as password recovery, account recovery, user registration, locking user accounts and password policies, etc. In this tutorial, we are going to try functionalities related to identity management in WSO2 Identity Server.

WSO2 IS Configurations

Configure the email server

1. Configure the email server to send emails by following the below steps.
    a. Open the `deployment.toml` file in the `<IS_HOME>/repository/conf` path.
    b. Specify values for the from_address, username, and password parameters in the `[output_adapter.email]` section as shown in the extract below:

```
[output_adapter.email]
from_address="<email>"
username="<email>"
password="<password>"
hostname="smtp.gmail.com"
port=587
enable_start_tls=true
enable_authentication=true
```

(if you are using a gmail account as the sender, create an App password

and use that as the password. If your password contains invalid characters such as “>” , “<” and “&”, enter the password as "<![CDATA[xxxx]]>")

2. Navigate to `<IS_HOME>/bin` and start the server by executing either of the following commands.

    Linux --> *`sh wso2server.sh`*

    Windows --> *`wso2server.bat`*

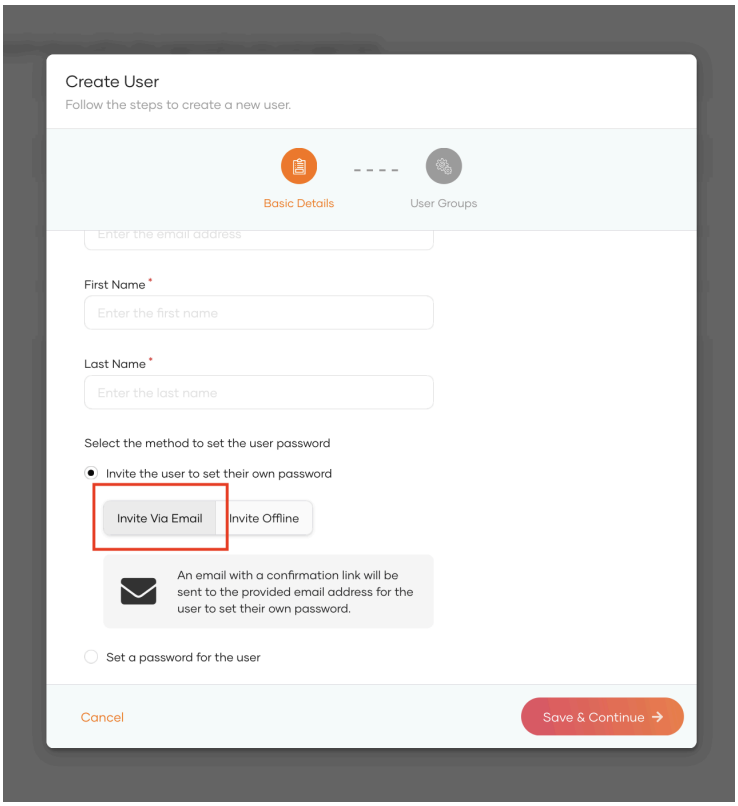
3. Log in to the Console App, and enter admin as both the username and the password.

Enable email invitations for user password setup

1. On the WSO2 Identity Server **Console menu bar,** click on the **Login & Registration** menu item.
2. When scrolled down a bit you will see the Invite User to Set Password option. Click on that.
3. From the given set of configuration check the box in front of **Enable email invitations for user password setup**.

Create a user

1. Expand the **User Management** menu item, click on **Users**.
2. On the **Users page**, click **Add User** and select **Single User** from the dropdown.
3. In the opened up wizard,
    - Keep **Primary** as the user store.
    - Add the below configuration to the respective fields.
        - Username: **tommy**
        - Email: **tommy@wso2.com**
        - First Name: **Tommy**
        - Last Name: **Dave**
4. Select **Invite the user to set their own password** option.
5. Select **Invite Via Email**.



6. Click **Next.**
7. Skip group selection and Click **Save & Continue**.
8. The user will receive an email to **tommy@wso2.com** with an invitation link to set the password.
9. Open the **Invitation link** received.
10. Add a **password** and confirm it.
    - Ex: **Tommy@123**

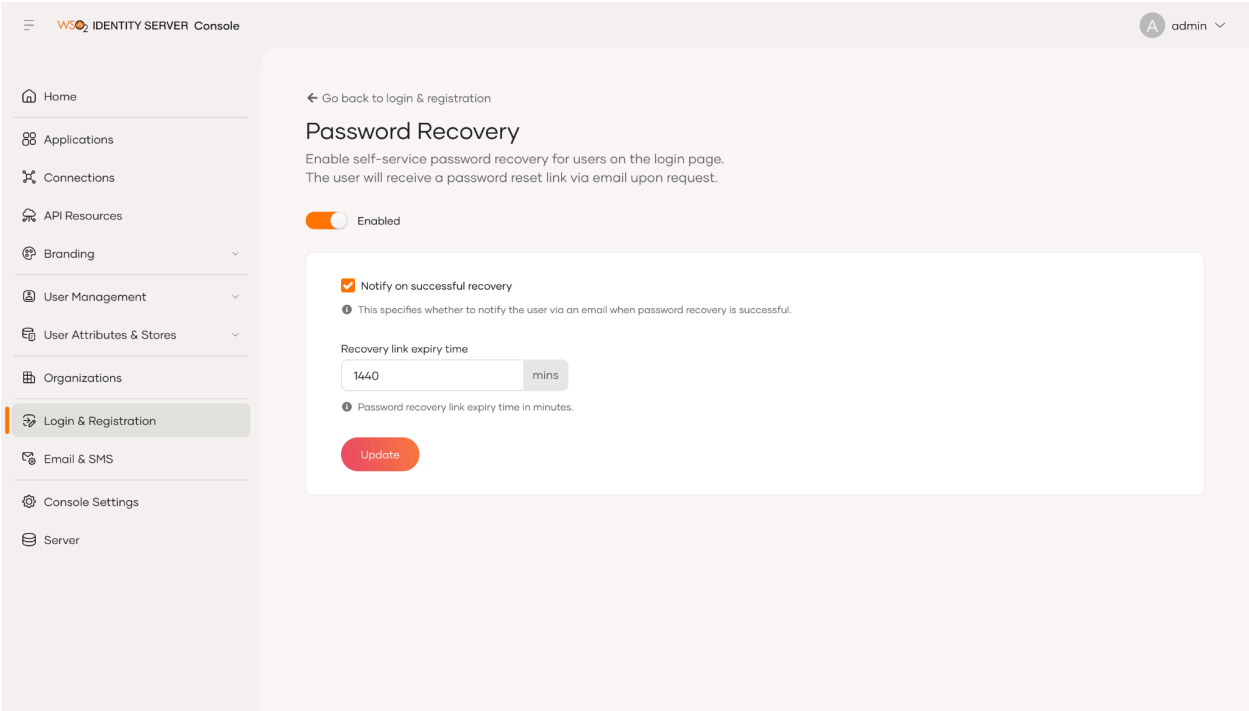
Password Recovery

Introduction:

In this section we will configure Email based password recovery option.

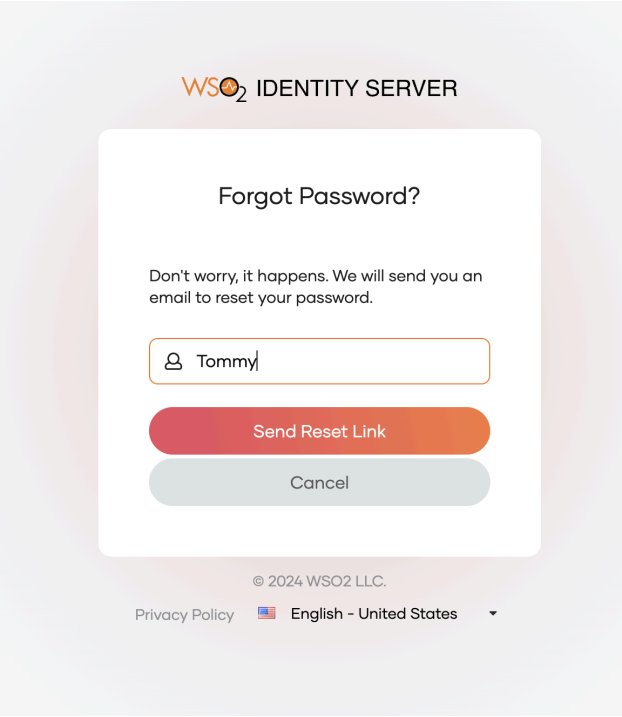
Setting up

1. In the WSO2 Identity Server **Console**, go to **Login & Registration** > **Account Recovery** > **Password Recovery.**
2. **Toggle** the switch to enable password recovery option to allow users to recover their passwords.
3. **Check Notify on successful recovery** to send a confirmation email upon successful password reset.
4. Click **Update** to save the changes.

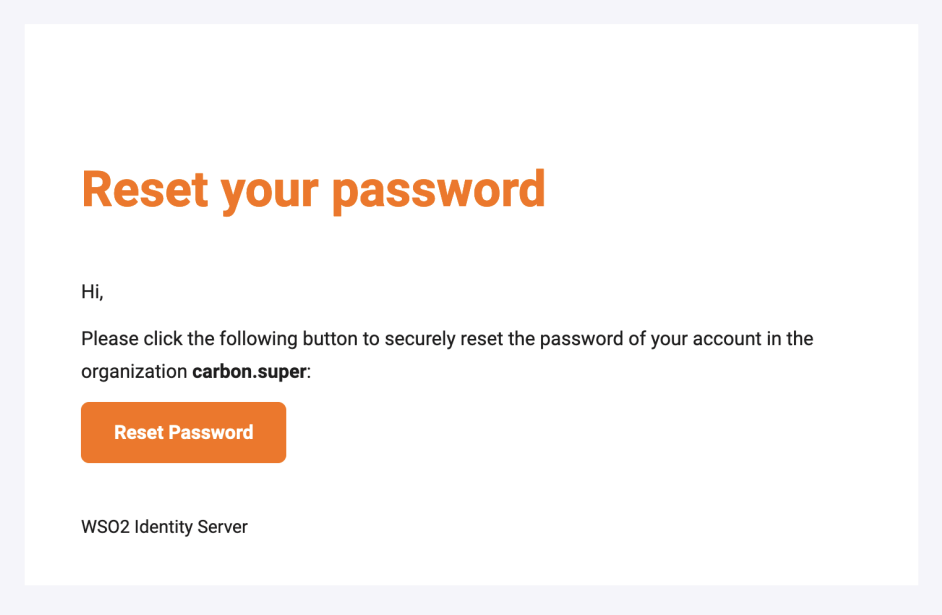


Try It

1. Go to My Account.
2. Click the **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.



5. An email notification is sent to the user's email address. Click on the **Reset Password** button in the email.



6. Enter a new password and click **Submit**.

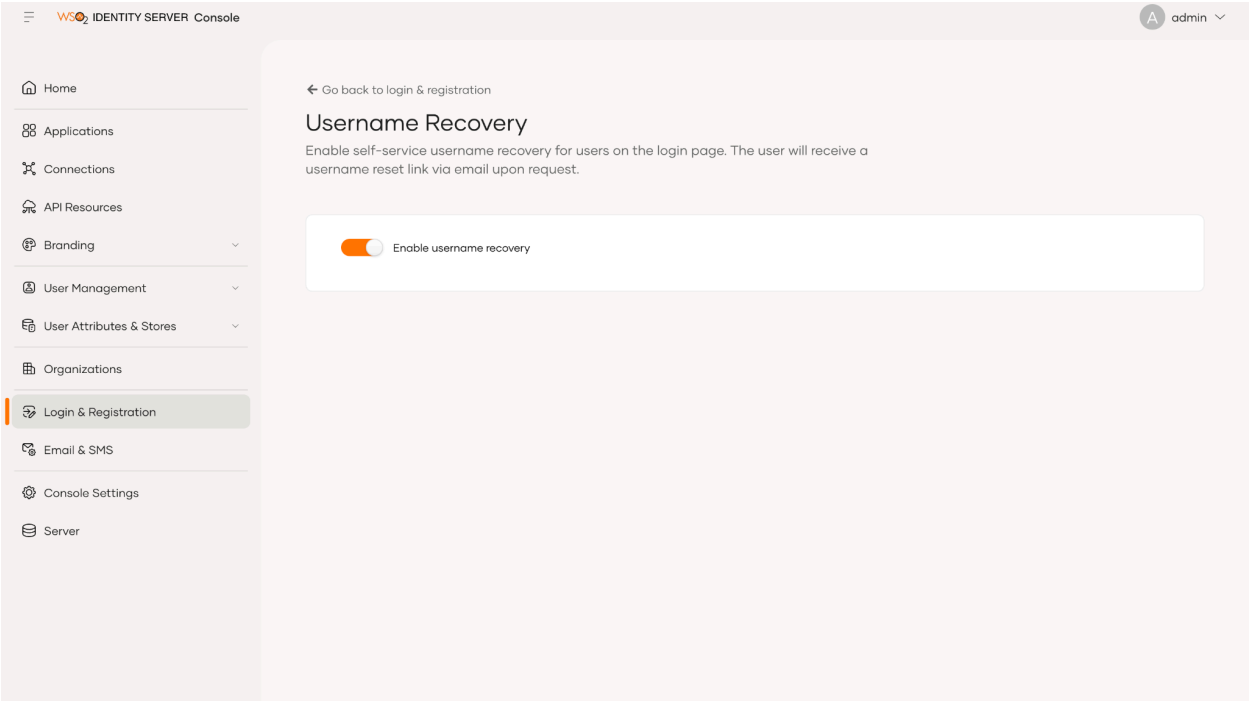
Username Recovery

Introduction:

In this section we will configure email based username recovery.

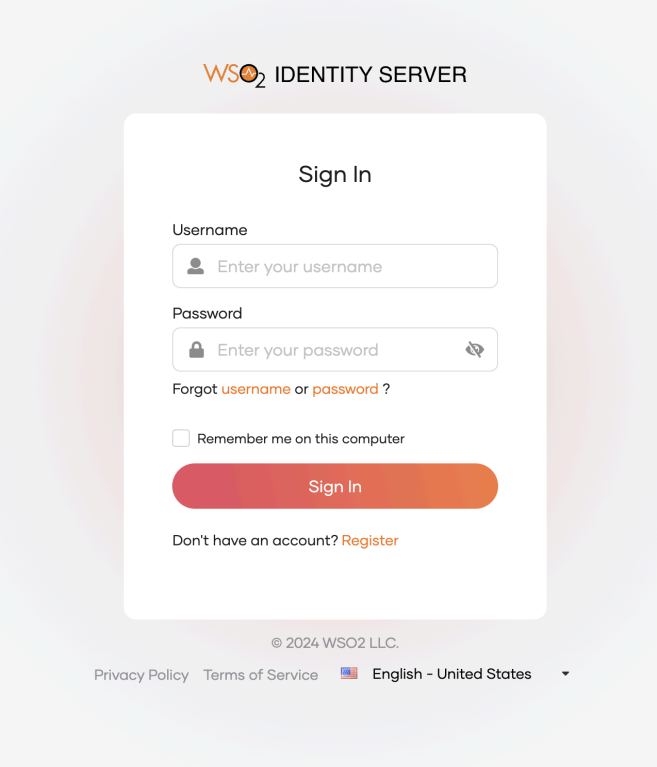
Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration** > **Account Recovery** > **Username Recovery.**
2. **Toggle** the switch to enable the username recovery option to allow users to recover their passwords.

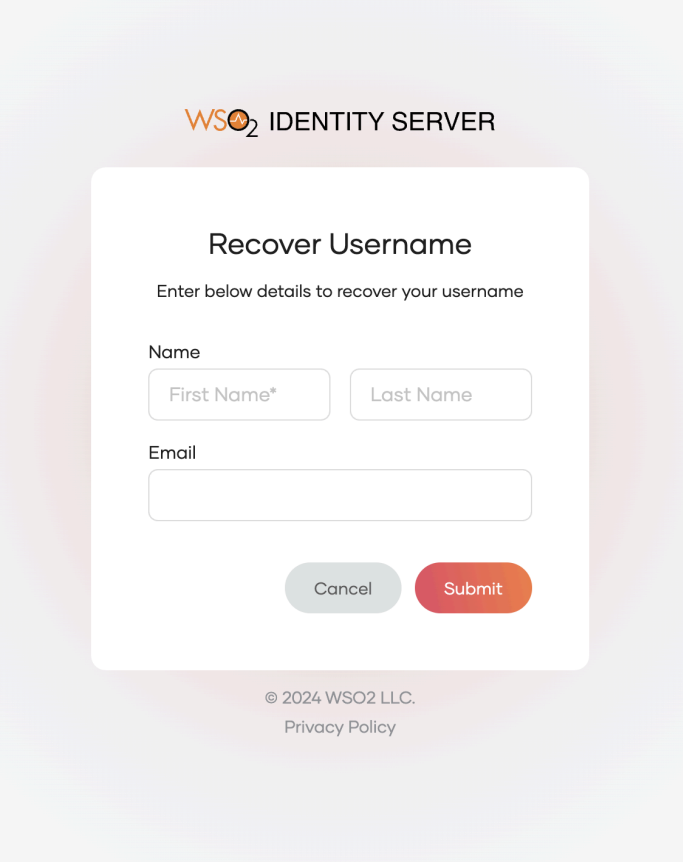


Try It:

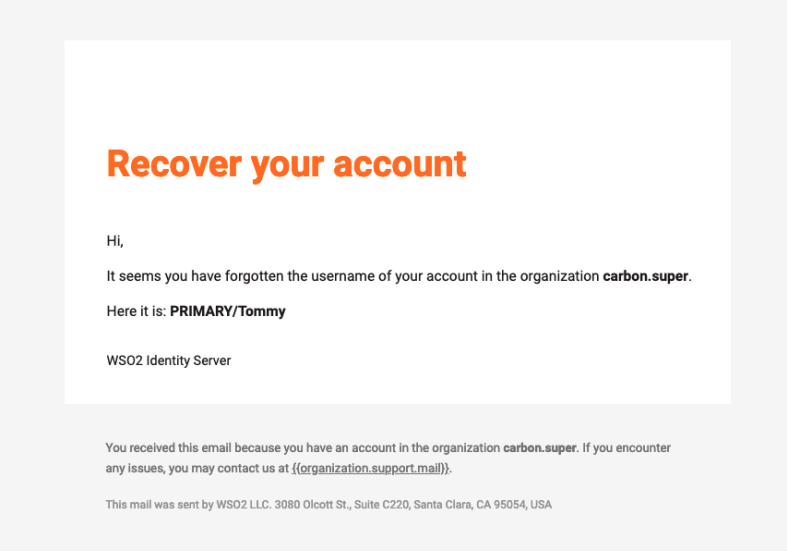
1. Go to My Account.
2. Click **Forgot username**.



3. Enter all the required fields and click **Submit**.



4. An email notification will be sent to the user's email address with the recovered username.



Account Locking

Introduction

The account locking feature is used to temporarily block a user from logging in. Account locking can be done by an administrative user or it can be configured to automatically lock upon multiple failed login attempts.

Setting up:

1. To show more specific error messages on the login page, the following property can be configured in the `deployment.toml` file in `<IS_HOME>/repository/conf` path.

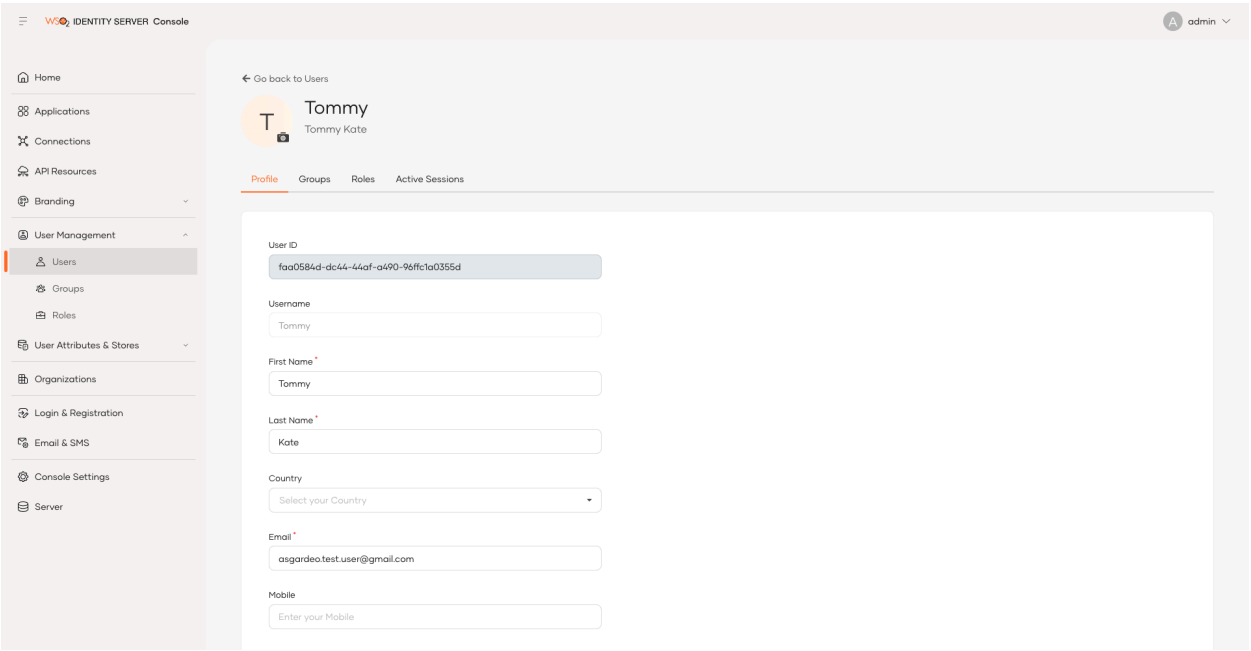
```
[authentication.authenticator.basic.parameters]
 showAuthFailureReason=true
 showAuthFailureReasonOnLoginPage=true
```

2. **Restart** the server.

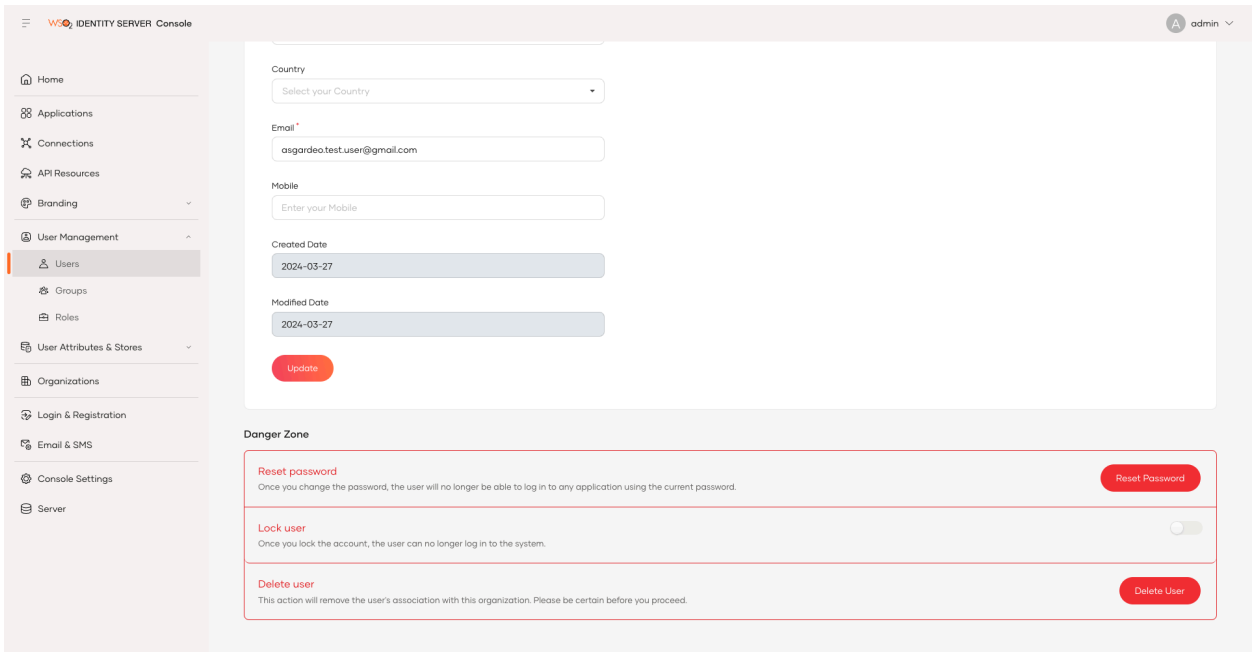
Account Locking by an administrator

Setting up:

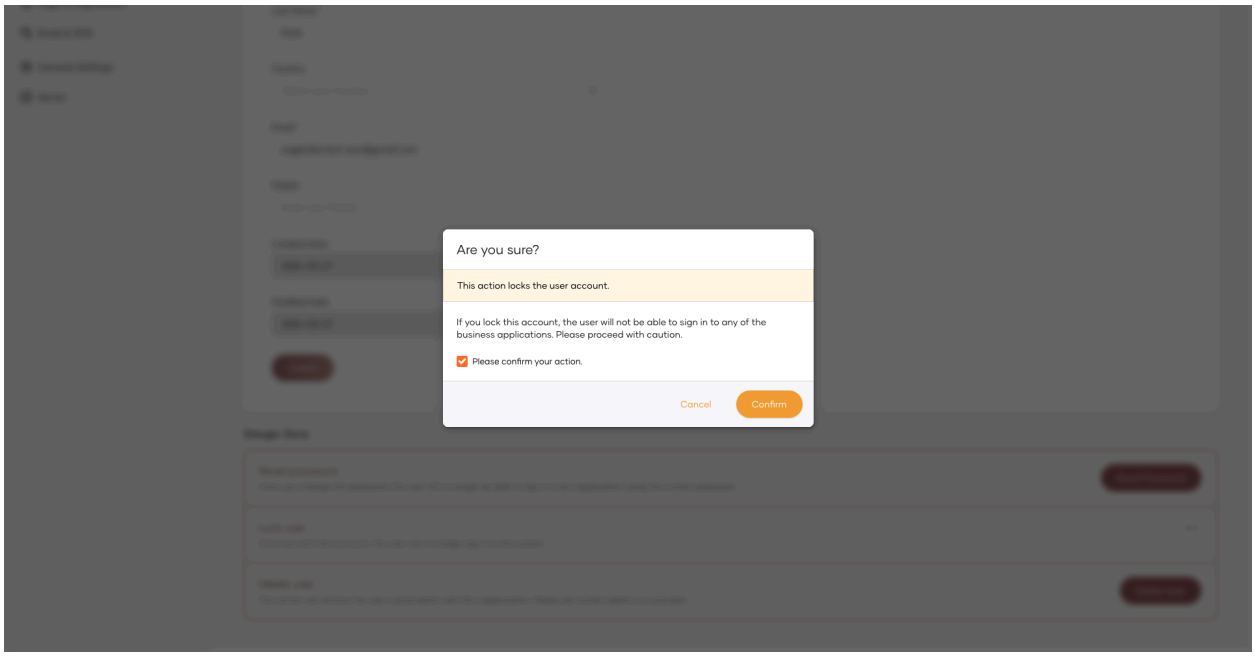
1. On the WSO2 Identity Server **Console**, expand the **User Management** menu item, click on **Users.**
2. Select the user **Tommy**.



3. Toggle the button on **Lock user** option at the bottom of the page.

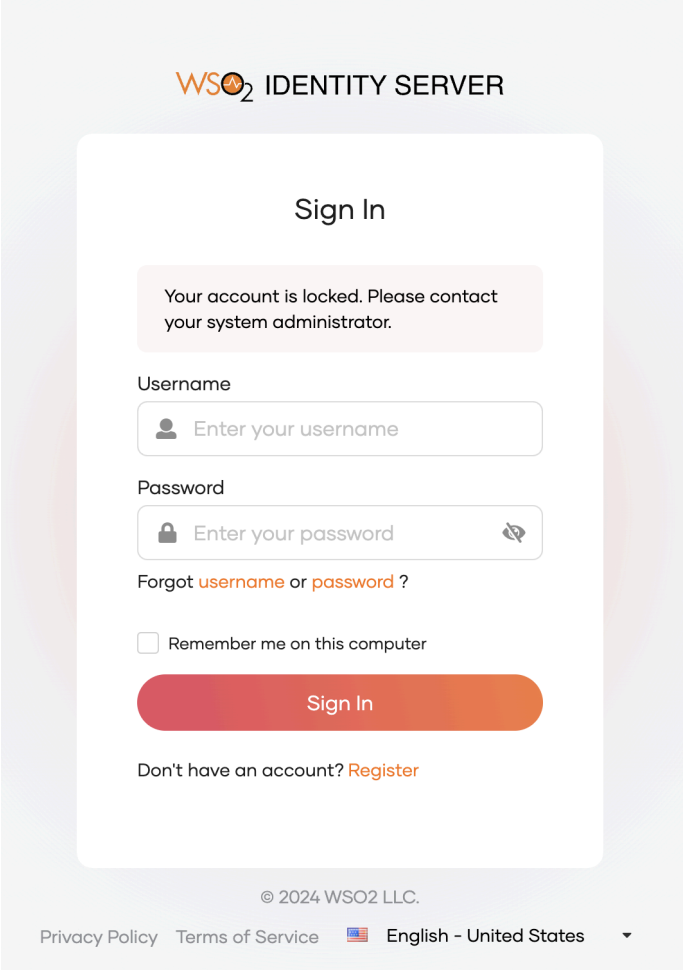


4. Check the **Please confirm your action** check box in the pop up.



Try It:

1. Go to My Account, and try to login as the user you locked.
2. Now the login attempt will fail.

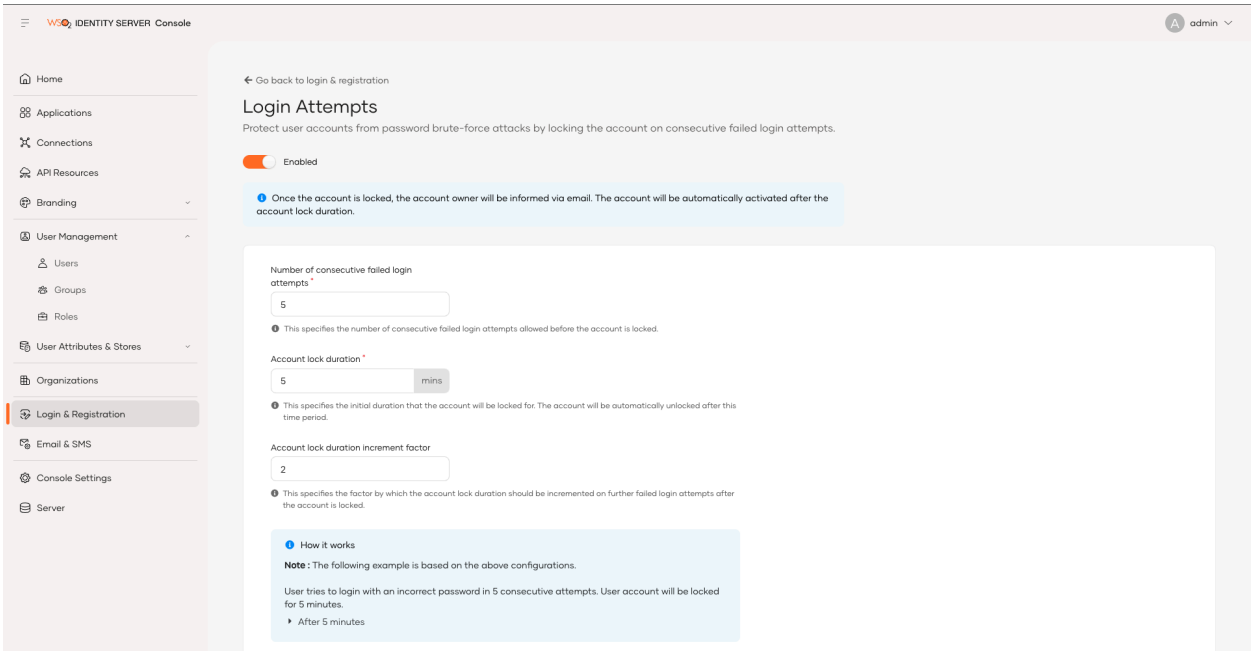


3. An email notification will be sent to the user's email address mentioning the account has been locked.

Account Locking based on failed login attempts

Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration** > **Login Security** > **Login Attempts**
2. **Toggle** the switch to enable lock user accounts on failed attempts.



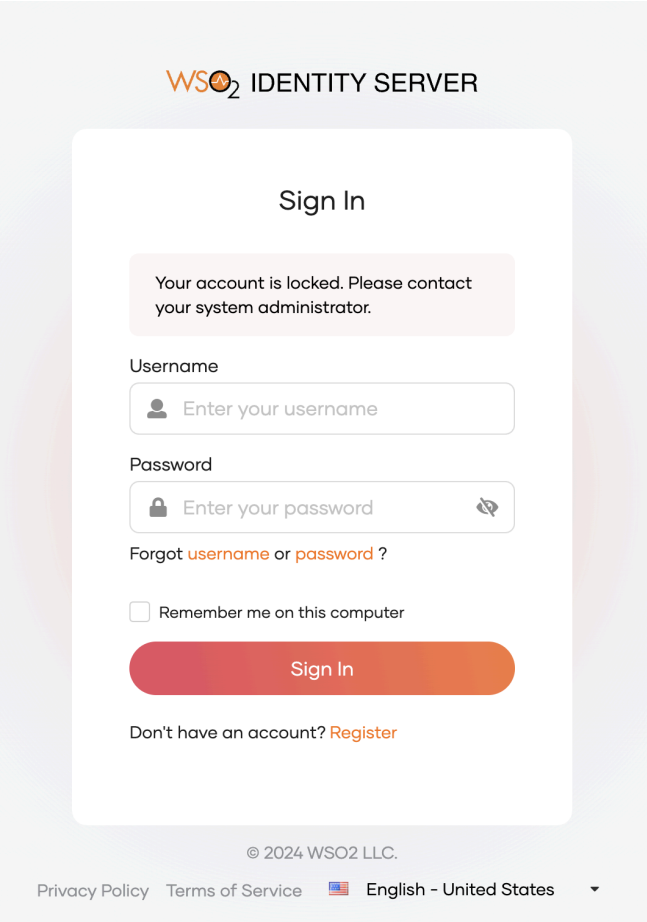
3. Specify Maximum failed login attempts as follows.

   Maximum failed login attempts: 3

4. Click **Update**.

Try It:

1. Go to My Account, and try to login giving wrong passwords 3 times.
2. Now try to login using actual credentials. Now your login attempt will fail as the account got locked.
3. An email that informs about the account locking is sent to the given email address.



4. Wait for 5 minutes and try to log in again with the correct credentials. The WSO2 Identity Server Dashboard home screen appears.

Password Policies

Password Policies are some set of rules that enhance the users to use strong passwords. WSO2 Identity server helps you to customize password patterns so as to enforce stronger password policies.

Password Input Validation

Introduction

Password input validation involves checking the validity of passwords entered by users against certain criteria or rules in real-time. Using this feature, organizations can enforce the users to input passwords that meet the required length, complexity, and other specified criteria for passwords.

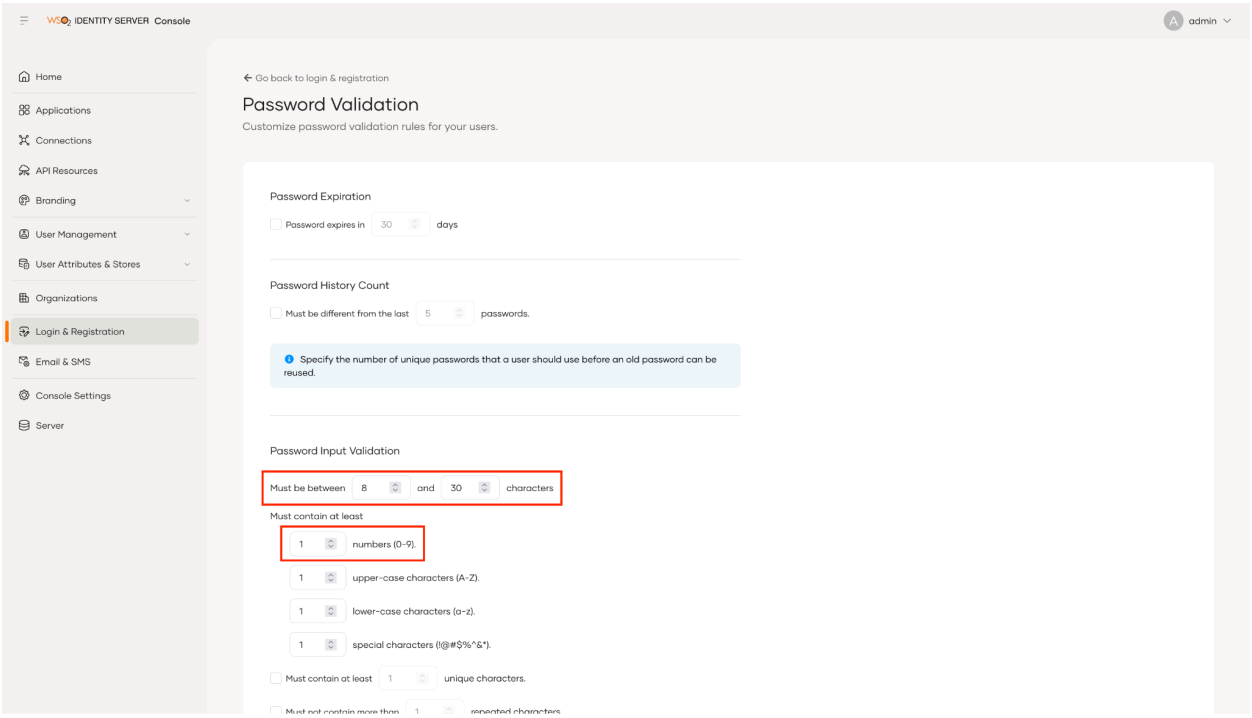
Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration** > **Login Security** > **Password Validation.**

2. Adjust password policies accordingly. Change the following fields.

    Password Input Validation

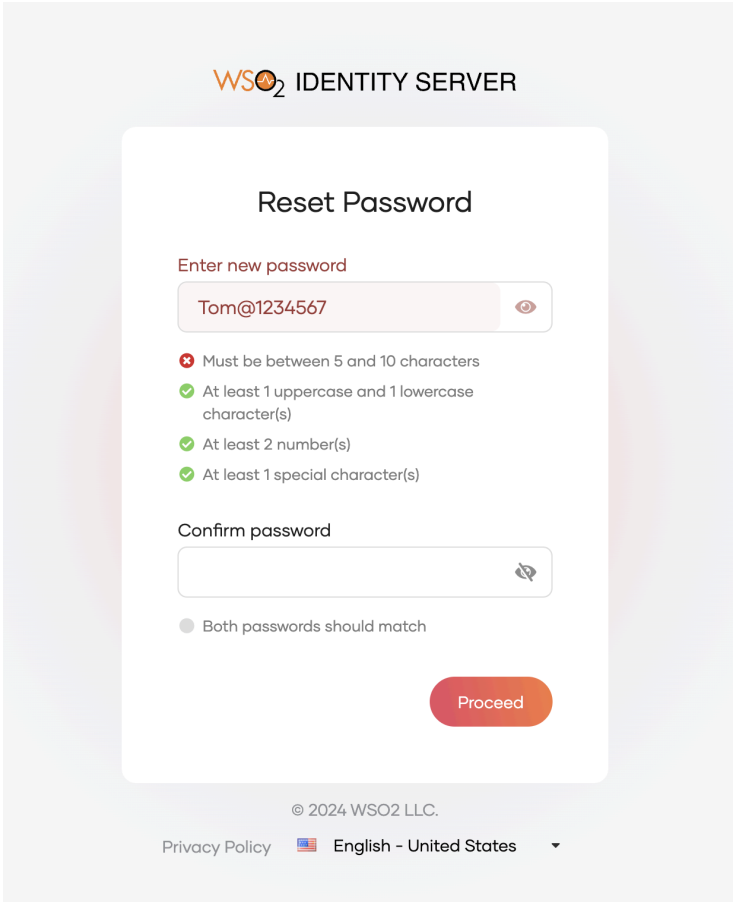
    - Must be between **5** and **10** characters
    - Must contain at least **2** numbers (0-9).



3. Click **Update.**

Try It:

1. Access the WSO2 Identity Server dashboard using the following link: My Account
2. Click **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.
5. An email notification is sent to the user's email address. Click on the **Reset Password** button given on the email.
6. Enter a password which violates the password patterns specified. It will give the error specified. Ex: Tom@1234567


WSO2 IDENTITY SERVER
Reset Password
Enter new password
Tom@1234567
Must be between 5 and 10 characters
At least 1 uppercase and 1 lowercase character(s)
At least 2 number(s)
At least 1 special character(s)
Confirm password
Both passwords should match
Proceed
© 2024 WSO2 LLC.
Privacy Policy
English - United States

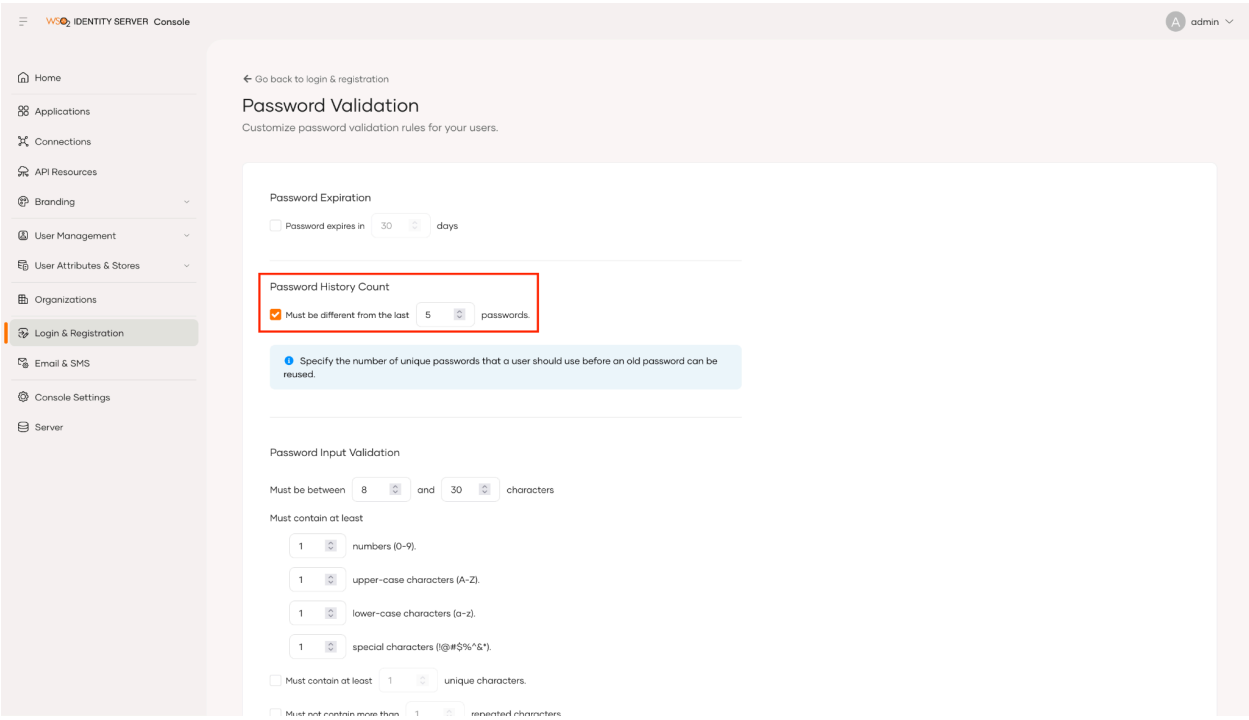
Password History

Introduction

This feature helps to prevent users from configuring passwords that were used in the recent past. For example, if you configure a count of 2 passwords, users will be prevented from reusing their last 2 passwords as the current password.

Setting up:

1. In the WSO2 Identity Server Console, go to **Login & Registration** > **Login Security** > **Password Validation.**
2. Under the **Password History Count** check the checkbox for the option that says **Must be different from last __ passwords**.
3. Add 1 as the number of passwords.



4. Click **Update**.

Try It:

1. Access the WSO2 Identity Server dashboard using the following link: My Account
2. Click **Forgot Password**.
3. Enter the user's username.
4. Click **Send Reset Link**.
5. An email notification is sent to the user's email address. Click on the **Reset Password** button given on the email.
6. Enter the existing password. It will give the error specified. Ex: **Tom@1234**